IMT3491 Ethical Hacking and Penetration Testing - 2015-2016

Emnekode:
IMT3491

Emnenavn:
Ethical Hacking and Penetration Testing

Faglig nivå:
Bachelor (syklus 1)

Studiepoeng:
5

Varighet:
Høst

Språk:
Engelsk

Forutsetter bestått:
IMT2282 Operating systems

Anbefalt forkunnskap:
Master students must document that they have achieved learning outcomes equivalent to IMT2282 Operating systems

Forventet læringsutbytte:
Knowledge:

- Explain how a penetration test is planned, executed, documented and terminated.
- Account for vulnerabilities in general and common services running on internal and external servers for a generic company.
- Predict client side vulnerabilities and use the new methods for security breaches that may occur here.

Skills:

- Master the most common hacking and penetration testing tools and apply these tools to perform simple penetration testing tasks.
- Carry out structured and effective search for security issues in computer systems and computer networks.
- Construct effective penetration tests given existing threats towards software, networks, and network services.
- Use and abuse access to one system in order to gather more information about the networks and services used by this system.

General competence:

- Awareness of vulnerabilities in software both at server and client side, with an extra focus on network applications.
- Sensitivity for potential vulnerabilities in the computer systems and networks of a generic company, and ability to make an analysis of potential threats based on a network description.
- Overview of a wide set of tools for testing and accessing systems and networks.

Emnets temaer:

- Ethical hacking and penetration testing – definitions
- Penetration testing methodologies
- Hands-on penetration testing

Pedagogiske metoder:
Forelesninger
Gruppearbeid
Lab.øvelser
Oppgaveløsning

Pedagogiske metoder (fritekst):
The course will be made accessible for both campus and remote students. Every student is free to choose the pedagogic arrangement form that is best fitted for her/his own requirement. The lectures in the course will be given on campus and are open for both categories of students. All the lectures will also be available on Internet through GUC's learning management system (Fronter).

Vurderingsformer:
Skriftlig eksamen, 2 timer
Vurdering av prosjekt(er)
Digital eksamen (leveringsform se tekstfelt)

Vurderingsformer:

- Digital OR written exam, (66%), depending on the number of students the exam might be oral
- Project (34%)
- Both parts must be passed

Karakterskala:
Bokstavkarakterer, A (best) - F (ikke bestått)

Sensorordning:
Evaluated by internal examiner. External examiner is used periodically (every four years, next time in 2014/2015).

Utsatt eksamen (tidl. kontinuasjon):

- No re-sit examination – projects and exam are closely connected and related
- New project(s) and exam at next course dates

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
None.

Obligatoriske arbeidskrav:
One or two approved exercises, further information announced at course start.

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig kobling:
Basel Katt

Emneansvarlig:
Basel Katt

Læremidler:
Engebretson, P. (2013). The Basics of Hacking and Penetration Testing 2nd Ed.

Supporting literature

Regalado, D., Harris, S., Harper, A., Eagle, C., Ness, J., Spasojevic, B., Linn, R., Sims, S. (2015): Gray Hat Hacking The Ethical Hacker's Handbook 4th Ed.

Supplerende opplysninger:
In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not an if yes, in which form.

There will also be an upper limit to the class based on available laboratory resources.

Klar for publisering:
Ja